On the Shortest Identity in Finite Simple Groups of Lie Type

Uzy Hadad

March 18, 2010

Abstract

We prove that the length of the shortest identity in a finite simple group of Lie type of rank r defined over $\mathbb{F}_q$, is bounded (from above and below) by explicit polynomials in q and r.

1 Introduction

Let F_∞ be the free group on a countable number of generators and let w be a non-trivial reduced word in F_∞ on k generators, say $w = w(x_1, ..., x_k)$. Given a group G we say that w is an *identity*, or a *law*, for G, if $w(g_1, ..., g_k) = 1$ for every $(g_1, ..., g_k) \in G^k$. We denote by $\alpha(G)$ the length of the shortest identity of the group G (on any number of generators).

Let $\mathbb{F}_q$ be the finite field with q elements, where $q = p^m$ is a prime power, and let G be a finite simple group of Lie type over $\mathbb{F}_q$ of rank r. Here, if G is untwisted, r is the rank of the ambient simple algebraic group, while we define r for the twisted groups as follows (see [Car, Sec. 13.1] and also [GLS, Prop. 2.3.2]):

type	${}^2A_{2d}$	${}^2A_{2d-1}$	${}^2D_{d+1}$	${}^3D_4$	${}^2E_6$	${}^2F_4$	${}^2G_2$	${}^2B_2$
rank	d	d	d	2	4	2	1	1

Let $q^*(G)$ be the number of elements of the field where the group G is realized. For example, $q^*(A_n(q)) = q$, $q^*({}^3D_4(q)) = q^3$ and $q^*({}^2A_{2d}(q)) = q^2$. See Section 1.1 for more details.

The main result of this paper is the following:

Theorem 1. *Let G be a finite simple group of Lie type over $\mathbb{F}_q$ of rank r. Then the length of the shortest identity of G satisfies*

$$\frac{q^*(G)^{\frac{r}{4}} - 1}{3} \leq \alpha(G) < (31r + 2)^3 q^{31r}.$$

Furthermore, we give an explicit construction of an identity of length less than the upper bound.

In the case of $G = A_d(q) = PSL_{d+1}(q)$ we give a more precise statement, and then deduce Theorem 1 from this special case. Indeed, we prove the following:

Theorem 2. *The length of the shortest identity of $A_d(q)$ satisfies*

$$\frac{q^{\lfloor \frac{d+1}{2} \rfloor} - 1}{3} \leq \alpha(A_d(q)) < (d+3)^2 d q^{d+1}.$$

Furthermore, we give an explicit construction of an identity of length less than the upper bound.

In particular, Theorem 2 improves a result of Gamburd et. al. [GHSSV, Prop. 11] which states that $\alpha(SL_2(p)) \geq c \frac{p}{\log p}$ for some constant c.

The proof of Theorem 1 is based on the fact that if G is a finite simple group of Lie type over $\mathbb{F}_q$ (with the exception of Suzuki group) then there exists two positive integers c_1 and c_2, which depend only on the type and the rank of G, such that

$$A_1(q^{c_1}) \leq G \leq A_{c_2}(q).$$

Now since an identity of a group is inherited by its subgroups, we observe that Theorem 1 follows from Theorem 2.

Remark 1.1. If a group G is a central extension of a group Z by H(i.e $H = G/Z$), then if a word $1 \neq w(x_1, ..., x_k) \in F_\infty$ is an identity of H then it is easy to check that the word $[w, x_{k+1}] \in F_\infty$ is also an identity of G. Furthermore, if $1 \neq w(x_1, ..., x_k) \in F_\infty$ is an identity of G then it is an identity of H. Therefore we obtain similar results for quasisimple groups.

Let F_k be the free group on k generators $x_1, ..., x_k$. Given a word $w(x_1, ..., x_k) \in F_k$ we define $l(w)$ to be the length of w. Let $1 \neq w \in F_k$ be an identity for a finite group G and let $S = \{g_1, ..., g_k\} \subset G$. Then starting at any vertex in the Cayley graph $Cay(G, S)$, the walk $w(g_1, ..., g_k)$ is a closed walk of length $l(w)$. Hence in some sense, $\alpha(G)$ is a universal girth of the Cayley graphs of the group.

Recently there has been great interest in the study of word maps in finite simple groups and in algebraic groups (see [Lar, LS, NS1, Sh]). Let $w = w(x_1, ..., x_k)$ be a non-trivial word in F_k, where $k \geq 1$, and let G be a group. We define

$$w(G) = \langle w(g_1, ..., g_k) : (g_1, ..., g_k) \in G^k \rangle.$$

The next result follows immediately from Theorem 1 (since the hypothesis on $l(w)$ implies that $w(G)$ is a non-trivial normal subgroup of G).

Corollary 1. *Let G be a finite simple group of Lie type over $\mathbb{F}_q$ of rank r, and let $w \in F_k$ be a non-trivial word with $l(w) < \frac{q^*(G)^{\frac{r}{4}} - 1}{3}$, where $k \geq 1$. Then $w(G) = G$.*

1.1 Notation and Definitions

Let G be group, for every $g, h, \in G$ we define $g^h = hgh^{-1}$ and $[g,h] = ghg^{-1}h^{-1}$. In case G is finite, we write $exp(G)$ for the exponent of G. In addition, for an element $g \in G$ we define $ord(g)$ to be the order of g. For $x \in \mathbb{R}$ we write $\lfloor x \rfloor$ for the greatest integer less than or equal to x.

The untwisted groups $A_d(q), B_d(q), C_d(q), D_d(q), E_6(q), E_7(q), E_8(q), F_4(q), G_2(q)$ are realized over the finite field $\mathbb{F}_q$. The twisted groups

$$^2A_{2d}(q), {}^2A_{2d-1}(q), {}^2D_{d+1}(q), {}^3D_4(q), {}^2E_6(q),$$

are realized over finite fields with q^2, q^2, q^2, q^3, q^2 elements respectively, and the Ree and Suzuki groups ${}^2F_4(q), {}^2G_2(q), {}^2B_2(q)$, are realized over finite fields with $q = 2^{2n+1}, q = 3^{2n+1}, q = 2^{2n+1}$ elements respectively (see [Car, ch. 13.]).

We shall not go into further details about the structure and construction of finite simple groups of Lie type, we refer the reader to the book of Carter [Car] which is our main reference (see also [GLS]).

2 Previous Work

A *variety* of groups is a class of groups that satisfy a given set of laws (see [Ne, ch. 1]). By Birkhoff's theorem [Be] each variety $\mathfrak{B}$ is defined by a suitable set of words $B \subseteq F_\infty$, that is, $\mathfrak{B}$ consists of all the groups G on which $w(g_1, ..., g_k) = 1$ holds for each word $w(x_1, ..., x_k) \in B$ and for each set of elements $g_1, ..., g_k \in G$.

For example the variety which is defined by the law

$$\{[x_1, x_2] = x_1x_2x_1^{-1}x_2^{-1} = 1\},$$

is the abelian groups. In the language of varieties, the main aim of this paper is to study the length of the shortest law in the variety which is generated by all the laws in a finite simple group of Lie type.

In the 1960's, various papers were written on varieties of groups, which were mainly concerned with their qualitative properties. The most notable contribution is Hanna Neumann's book [Ne]. In this book, she raised ([Ne, p. 166]) the following question:

> *Is there a law which is satisfied in an infinite number of non-isomorphic non-abelian finite simple groups?*

G. A. Jones [Jon] gave a negative answer to this question, but his proof does not give an explicit bound on the length of the shortest identity in each family of finite simple groups of Lie type (except for the case of Suzuki groups). Our work can be thought of as a quantitative version of Jones's results.

A *basis* for a variety $\mathfrak{B}$ is a set of laws such that its closure is $\mathfrak{B}$ (for the definition of 'closure', see [Ne, ch. 1]). Oates and Powell in [OP] proved that every variety generated by a finite group has a finite basis. It is clear that if we know a basis for the variety generated by the laws in a given group G, then the minimum length of a law in this basis, is an upper bound for the shortest identity of the group.

In the literature a few attempts have been made to find an explicit basis for the variety generated by a finite non-abelian simple group. J. Cossey and S. Macdonald [CM] gave a finite basis for the set of laws in $PSL_2(5)$, and this was extended in [CMS] to $PSL_2(p^n)$ with $p^n \leq 11$. B. Southcott [So1, So2] gave a basis for the family $PSL_2(2^n)$, but the length of each element in his basis is greater than the upper bound of the shortest identity we state in Theorem 2.

Let $\mathcal{X}$ be any infinite set of groups. A group G is said to be *residually* $\mathcal{X}$, if for every $1 \neq g \in G$ there exists an epimorphism φ from G to some $H \in \mathcal{X}$ such that $\varphi(g) \neq 1$.

Suppose that the free group on k generators F_k is residually $\mathcal{X}$, and for a given group $H \in \mathcal{X}$ we can determine the maximal length of a non-trivial word w in F_k such that there exists an epimorphism φ from F_k to H with $\varphi(w) \neq 1$. Then this gives a lower bound on the length of the shortest identity (on k generators) in H.

W. Magnus [Ma, p. 309] raised the following related problem:

> *Let $\mathcal{X}$ be any infinite set of non-abelian finite simple groups. Is the free group F_k on $k \geq 1$ generators residually $\mathcal{X}$?*

T. Weigel [We1, We2, We3] gave a complete answer to this question. From his proof, we can conclude that in the case of a classical simple group G over $\mathbb{F}_q$ where $q = p^m$ is a prime power, the length of the shortest identity (on two generators) is at least p, and for the exceptional groups $E_6(q), E_7(q), E_8(q), G_2(q), F_4(q)$ and the twisted groups ${}^3D_4(q), {}^2E_6(q), {}^2F_4(q)$, the length of the shortest identity (on two generators) is at least $\log q$. Weigel's work involves 'identities' on two generators (and their inverses) of the group; in this paper we consider identities on any number of elements of the group (not necessarily generators).

3 Proof of Theorem 2

3.1 The Upper Bound

In this section we give an explicit construction of an identity for the group $SL_n(q)$ and this gives the upper bound stated in Theorem 2. This construction is based on the exponent of the group.

Lemma 3.1. *Let $q = p^f$ where p is a prime. Then the exponent of $SL_n(q)$ is*

$$p^e \cdot lcm[q-1, q^2-1, ..., q^{n-1}-1, \frac{q^n-1}{q-1}],$$

where e is the minimal positive integer such that $p^e \geq n$.

Proof. Let $x \in GL_n(q)$ be a non-trivial element. Write $x = x_s \cdot x_u$ in Jordan form, where $x_u \in GL_n(q)$ is unipotent, $x_s \in GL_n(q)$ is diagonalizable over a splitting field $\mathbb{F}_{q^r}(r \leq n)$ and $[x_s, x_u] = 1$. Here $ord(x_u)$ is a power of p, while $ord(x_s)$ is coprime to p.

Suppose $x_u = 1$. Then x is diagonalizable over $\mathbb{F}_{q^r}$, and therefore $x^{q^r-1} = x_s^{q^r-1} = 1$. Furthermore, for every $1 \leq j \leq n$, there exists an element in $GL_n(q)$ of order $q^j - 1$. This follows from the fact that the field $\mathbb{F}_{q^j}$ can be considered as a vector space over $\mathbb{F}_q$ of dimension j. Take a generator of the cyclic group $\mathbb{F}_{q^j}^*$; it is of order $q^j - 1$ and it acts as a linear transformation on $\mathbb{F}_q^j$, hence it belongs to $GL_n(q)$.

Now suppose x_u is non-trivial and let $m = ord(x)$. Then $x_s^m x_u^m = 1$ since $[x_s, x_u] = 1$, so m is divisible by $ord(x_s)$ and $ord(x_u)$.

Now every unipotent matrix x_u can we written as $x_u = 1 + N$, where 1 is the identity matrix in $GL_n(q)$ and N is an $n \times n$ nilpotent matrix over $\mathbb{F}_q$. For every $i \in \mathbb{N}$, we have $x_u^{p^i} = (1+N)^{p^i} = 1 + N^{p^i}$. Let e be the minimal positive integer such that $p^e \geq n$. Then it is easy to check that p^e is the exponent of the upper unitriangular matrices in $GL_n(q)$, and there exists a unipotent matrix in $GL_n(q)$ with this order.

For $SL_n(q)$ all the above holds except for the fact that the maximal order of an element in $SL_n(q)$ is $\frac{q^n-1}{q-1}$ and not $q^n - 1$ as in $GL_n(q)$. □

Remark 3.2. There exists a constant c such that $exp(SL_n(q)) \geq q^{cn^2}$ (see [BMP, Lemma 2.3] and the discussion afterward). Thus our bound in Theorem 2 is shorter than the length of the exponent identity $x^{exp(SL_n(q))}$.

Lemma 3.3. *Let G be a group and let $w_1, ..., w_m$ be distinct non-trivial power-words in one variable in the free group F_{k+1} on $k+1$ generators $x_1, ..., x_{k+1}$ where $k = 2^{\lfloor \log_2 m \rfloor}$. Suppose that $l(w_1) \geq l(w_2) \geq ... \geq l(w_m)$ and that for each element $g \in G$, there exists some i such that $w_i(g) = 1$. Then there exists a non-trivial word $w \in F_{k+1}$ of length at most $4m^2(l(w_1)+1)$ which is an identity in G.*

Proof. For $1 \leq i \leq \lfloor \frac{m}{2} \rfloor$, set $u_i = [w_{2i-1}(x_1), w_{2i}(x_1^{x_{i+1}})]$. If m is odd then set

$$u_{\lfloor \frac{m}{2} \rfloor + 1} = [w_m(x_1), x_{\lfloor \frac{m}{2} \rfloor + 2}],$$

else if m is even set

$$u_{\lfloor \frac{m}{2} \rfloor + 1} = [x_1, x_{\lfloor \frac{m}{2} \rfloor + 2}].$$

For $\lfloor \frac{m}{2} \rfloor + 2 \leq i \leq k$, set $u_i = [x_1, x_{i+1}]$. Let $j = 2^e$ for some positive integer $e \leq \lfloor \log_2 m \rfloor$, and define a recursive function f in the following way:

$$f(u_1, ..., u_{2^{e-1}}, ..., u_j) = [f(u_1, ..., u_{2^{e-1}}), f(u_{2^{e-1}+1}, ..., u_j)]$$

and $f(u_i, u_{i+1}) = [u_i, u_{i+1}]$.

Let $w = f(u_1, ..., u_k)$. It is clear that w is a non-trivial word in F_{k+1} (since we have a new letter x_{j+1} in each u_j, which appears only in u_j). To show that w is an identity of G it is enough to note that x and x^y have the same order, hence at least one of the commutators in the expression for w collapses and hence so does the whole word.

Now since $w_i(x_1^{x_j}) = x_j w_i(x_1) x_j^{-1}$, the length of the word $[u_1, u_2]$ is at most $2^4 \cdot l(w_1) + 2^4$. By induction on e, since $l(w_1) \geq l(w_i)$ for all i, we get that the length of the word $f(u_1, ..., u_{2^e})$ is at most

$$2^{2(e+1)} l(w_1) + 2^{2(e+1)}.$$

Therefore, since $e \leq \lfloor \log_2 m \rfloor$, the length of w is at most

$$2^{2(\lfloor \log_2 m \rfloor + 1)} l(w_1) + 2^{2(\lfloor \log_2 m \rfloor + 1)} \leq 4m^2 l(w_1) + 4m^2 = 4m^2(l(w_1) + 1).$$

□

Proposition 3.4. *Let $q = p^f$ be a prime power and let $G = SL_n(q)$ where $n \geq 2$. Then there exists an identity in G of length at most $(n+2)^2 p^e q^{n-1}$, where e is the minimal positive integer such that $p^e \geq n$.*

Proof. Following the proof of Lemma 3.1, every element $g \in G$ satisfies at least one of the following words:

$$X^{p^e \frac{q^n - 1}{q-1}}, X^{p^e(q^{n-1}-1)}, X^{p^e(q^{n-2}-1)}, ..., X^{p^e(q-1)}.$$

If g satisfies the first word, then it also satisfies $X^{\frac{q^n-1}{q-1}}$ since it has distinct eigenvalues in the splitting field $\mathbb{F}_{q^n}$, hence it is diagonalizable over $\mathbb{F}_{q^n}$. Now for every $i \in \mathbb{N}$, $q^i - 1$ divides $q^{2i} - 1$, therefore every $g \in G$ satisfies at least one of the following words (ordered in decreasing length):

$$w_1 = X^{p^e(q^{n-1}-1)}, w_2 = X^{\frac{q^n-1}{(q-1)}}, w_3 = X^{p^e(q^{n-2}-1)}, ..., w_{\lceil \frac{n+1}{2} \rceil} = X^{p^e(q^{\lceil \frac{n+1}{2} \rceil}-1)}.$$

Now set $m = \frac{n+2}{2}$. The result follows by Lemma 3.3. □

If w is an identity in the group G, it is easy to see that w is also an identity for every quotient of G. Hence the identity we construct in Proposition 3.4 holds for $A_{n-1}(q) = PSL_n(q)$, and this gives the upper bound in Theorem 2.

3.2 The Lower Bound

Lemma 3.5. *Let G be a finite group and w an identity of G. If $l(w) < exp(G)$, then $l(w)$ is even.*

Proof. Let $w = w(x_1, ..., x_k)$ be an identity in G on k elements. If $l(w)$ is odd, then there exists $1 \leq i \leq k$ such that the sum of the exponents of x_i appearing in w is odd. Hence if we set $x_j = 1$ for all $j \neq i$, we get a power-word of length less than $exp(G)$, a contradiction.

□

We start with the case $A_1(q) = PSL_2(q)$.

Lemma 3.6. *Let $G = PSL_2(q)$, then $\alpha(G) \geq \frac{q-1}{3}$.*

Proof. If q is even then $PSL_2(q) = SL_2(q)$. If q is odd then the group $PSL_2(q)$ is isomorphic to $SL_2(q)/\mathbb{Z}_2$. In any case, if $w \in F_k$ is an identity of $PSL_2(q)$, then it is immediate to check that w^2 is an identity of $SL_2(q)$. So it is enough to prove that the length of the shortest identity of $SL_2(q)$ is at least $\frac{2}{3}(q-1)$.

Let

$$u(t) = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}, \tau = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, h(\lambda) = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}$$

where $t \in \mathbb{F}_q$ and $\lambda \in \mathbb{F}_q^*$. From the Bruhat decomposition for $SL_2(q)$, every element $g \in SL_2(q)$ has a unique expression in one of the following forms (see [Car, Cor. 8.4.4]):

$$g = u(a)h(\lambda) \text{ or } g = u(b)h(\gamma)\tau u(c).$$

Suppose $w = w(x_1, ..., x_k)$ is a non-trivial reduced word in F_k of length l which is an identity of $SL_2(q)$. Since we are interested in deriving a lower bound, we may assume that l is less than $exp(SL_2(q))$ (see Lemma 3.1), so l is even by Lemma 3.5.

Let

$$M = \{a_i, b_i, c_i, \lambda_i, \gamma_i : 1 \leq i \leq k\}$$

be a set of independent commuting indeterminates over $\mathbb{F}_q$, and let

$$X_i = u(a_i)h(\lambda_i) \text{ and } Y_i = u(b_i)h(\gamma_i)\tau u(c_i).$$

Then X_i and Y_i are matrices with entries in $\mathbb{F}_q[M]$ and it is immediate to verify that the entries of

$$\lambda_i X_i, \gamma_i Y_i, \lambda_i X_i^{-1} \text{ and } \gamma_i Y_i^{-1}$$

are polynomials of degree at most 2 in the variables in M.

Let n_i be the sum of the moduli of the exponents of x_i appearing in w (for example if $w = x_1 x_2 x_1^{-1} x_2^{-1}$ then $n_1 = n_2 = 2$) and let I_2 be the identity matrix in $SL_2(q)$. For any $Z_i \in \{X_i, Y_i\}$, the matrix

$$C(Z_1, ..., Z_k) = \prod_{i=1}^{k} \beta(Z_i)^{n_i} (w(Z_1, ..., Z_k) - I_2)$$

where $\beta_i(X_i) = \lambda_i$ and $\beta(Y_i) = \gamma_i$, has entries in $\mathbb{F}_q[M]$ having degree at most $2n_i$ in each of the variables $a_i, b_i, c_i, \lambda_i, \gamma_i$.
Now there are two cases to consider:

(i) For all the substitutions of Z_i by X_i or Y_i we get $C(Z_1, ..., Z_k) = 0$.

(ii) There is a substitution $(Z_1, ..., Z_k)$ such that $C(Z_1, ..., Z_k) \neq 0$.

First let us consider case (i). Let K be the algebraic closure of $\mathbb{F}_q$. Since for every substitution $C(Z_1, ..., Z_k)$ is zero, we deduce that w is a law on $SL_2(K)$. For every $n \in \mathbb{N}$, $SL_2(K)$ has a subgroup isomorphic to $SL_2(q^n)$, hence we obtain a law for the infinite family $\{SL_2(q^n)\}_{n=1}^{\infty}$. But the main theorem of Jones [Jon] states that there is no law which is satisfied by an infinite family of non-abelian finite simple groups, a contradiction.

Now let us consider case (ii). Let $(Z_1, ..., Z_k)$ be a substitution such that the word $w(Z_1, ..., Z_k) - I_2$ is not zero. Decompose $w(Z_1, ..., Z_k)$ as a product of two words:

$$w(Z_1, ..., Z_k) = w_1(Z_1, ..., Z_k)w_2(Z_1, ..., Z_k)$$

where $w_1(Z_1, ..., Z_k)$ is a word of length $\frac{1}{2}l$ (recall that l is even). Let T be the matrix

$$T = \prod_{i=1}^{k} \beta(Z_i)^{n_i}(w_1(Z_1, ..., Z_k) - w_2(Z_1, ..., Z_k)^{-1}).$$

Then there is an entry $T_{i,j}$ for some $1 \leq i, j \leq 2$, which is not formally zero. Let $M_1 \subseteq M$ be the set of indeterminates appearing in $T_{i,j}$. Then $T_{i,j}$ is a polynomial in $|M_1|$ variables of degree at most $\frac{3l}{2}$. Recall that if f is a polynomial in $\mathbb{F}_q[M_1]$ with $deg(f) = d \geq 0$, then the equation $f = 0$ has at most $dq^{|M_1|-1}$ solutions in $\mathbb{F}_q^{|M_1|}$ (see [LN, Thm. 6.13]). Therefore $T_{i,j}$ has at most $\frac{3}{2}l \cdot q^{|M_1|-1}$ solutions, hence $l \geq \frac{2}{3}(q-1)$ (the $q-1$ factor is because $\lambda_i, \gamma_i \in \mathbb{F}_q^*$). $\square$

It is easy to see that $A_1(q^n) = PSL_2(q^n)$ is a subgroup of $A_{2n-1}(q) = PSL_{2n}(q)$ (this follows from the fact that a 2 dimensional vector space over $\mathbb{F}_{q^n}$, can be considered as a $2n$ dimensional vector space over $\mathbb{F}_q$), thus we obtain the following result:

Proposition 3.7. *Let $G = A_d(q)$ where $d \geq 1$. Then $\alpha(G) > \frac{q^{\lfloor \frac{d+1}{2} \rfloor}-1}{3}$.*

This completes the proof of Theorem 2.

4 Proof of Theorem 1

4.1 The Lower Bound

In this section we will show that if G is a finite simple group of Lie type of rank r, and G is not a Suzuki group (i.e. type ${}^2B_2$), then G contains $A_{r'}(q')$, where $q' \leq q^*(G)$ and $r' \leq r$. Therefore, using Theorem 2, we obtain a lower bound for the shortest identity of G. For the Suzuki groups we use a lemma of Jones.

4.1.1 Untwisted groups

Let $G \neq A_d(q)$ be a simple untwisted group of Lie type over $\mathbb{F}_q$. By considering the associated Dynkin diagram, it is clear that if G has rank d then G contains $A_{d-1}(q)$, so Theorem 2 implies that $\alpha(G) \geq \frac{q^{\lfloor \frac{d}{2} \rfloor}-1}{3}$.

4.1.2 Twisted groups

Ree Groups: It is known that ${}^2F_4(2^{2n+1})$ and ${}^2G_2(3^{2n+1})$ contains $A_1(3^{2n+1})$ and $A_1(3^{2n+1})$ respectively [Ti, Lh].
Suzuki groups: The following lemma is a quantitative version of a result of Jones.

Lemma 4.1. *The length of the shortest identity of ${}^2B_2(2^{2n+1})$ satisfies*

$$\alpha({}^2B_2(2^{2n+1})) \geq \frac{2^{2n}-1}{1+2^n}.$$

For the proof we refer the reader to [Jon, Lemma 5]). Although this quantitative result is not stated there explicitly, it follows immediately from the proof (in fact, one can improve this bound by decomposing the identity word in the same way we did in the proof of Lemma 3.6).

The twisted groups ${}^2A_d(q)$,${}^2D_d(q)$,${}^2E_6(q)$,${}^3D_4(q)$:
The Dynkin diagrams of type A_d, D_d, E_6 and D_4 admit symmetries of order $2, 2, 2$ and 3, respectively. The twisted groups ${}^2A_d(q)$,${}^2D_d(q)$,${}^2E_6(q)$ and ${}^3D_4(q)$ are subgroups of the untwisted groups $A_d(q^2), D_d(q^2), E_6(q^2), D_4(q^3)$, and they are fixed by an automorphism σ (of $A_d(q^2)$ etc.) which maps each root element $X_\alpha(t)$ to $X_{\alpha'}(t^q)$, where $\alpha \mapsto \alpha'$ is a symmetry of the root system and $t \mapsto t^q$ is a field automorphism. The automorphism σ has order $2, 2, 2, 3$ respectively.

By inspecting the Dynkin diagrams of type $A_{2d-1}, A_{2d}, D_d, E_6$ and D_4, together with the corresponding automorphisms and roots relations, one can show that each of the following groups G has a subgroup H as given in the following table (see also [Ni, Sec. 2]):

G	${}^2A_2(q)$	${}^2A_{2d-1}(q)$	${}^2A_{2d}(q), d > 1$	${}^2E_6(q)$	${}^3D_4(q)$
H	$A_1(q)$	$A_{d-1}(q^2)$	$A_{d-1}(q^2)$	$A_2(q^2)$	$A_1(q^3)$

We give the details in the case of ${}^2A_{2d-1}(q)$, a similar argument applies in each of the remaining cases. Let $\prod = \{\omega_1, ..., \omega_{2d-1}\}$ be a base for the root system of type A_{2d-1}. Now for every $t \in \mathbb{F}_{q^2}$ and for every $1 \leq i < d$ the element $X_{\omega_i}(t)X_{\omega_{2d-i}}(t^q)$ is fixed by the automorphism σ and for every $t \in \mathbb{F}_q$ the element $X_{\omega_d}(t)$ is fixed by σ. It is well-known fact that if $|i-j| > 1$ then the root subgroups X_{ω_i} and X_{ω_j} commute, thus we get that the subgroup

$$H = \langle X_{\omega_i}(t)X_{\omega_{2d-i}}(t^q) : 1 \leq i < d, t \in \mathbb{F}_{q^2} \rangle$$

is isomorphic to $A_{d-1}(q^2)$.

So for a twisted group G in the above table with rank r, we deduce from Theorem 2 that the shortest identity of G has length at least $\frac{(q^*(G))^{\frac{r}{4}}-1}{3}$.

The only case left is ${}^2D_{d+1}(q)$ (recall that the rank of ${}^2D_{d+1}(q)$ is d). Let $n = 2^k$ for some integer $k \geq 2$ and fix d such that $n \leq d+1 < 2n = 2^{k+1}$. Then we have ${}^2D_{d+1}(q) \geq {}^2D_{\frac{n}{2}}(q^2) \geq A_1(q^n)$ (see [KL, Table 3.5.F]). Now since $2(\frac{d}{4}) < n$, we deduce that the shortest identity of ${}^2D_{d+1}(q)$ has length at least $\frac{q^n-1}{3} > \frac{(q^2)^{\frac{d}{4}}-1}{3}$.

4.2 The Upper Bound

In this final section we show that there exists a constant c such that every finite simple group of Lie type over $\mathbb{F}_q$ of rank r is isomorphic to a subgroup of $PSL_{cr}(q)$ or $SL_{cr}(q)$, and so the desired upper bound follows from Proposition 3.4.

Each finite simple group of Lie type can be constructed (see [Car, ch. 4]) as a subgroup of the automorphism group of the corresponding Lie algebra. In the following table we give the dimension of the Lie algebra $\mathfrak{g}$ in terms of the untwisted Lie rank:

$\mathfrak{g}$	A_d	B_d	C_d	D_d	E_6	E_7	E_8	F_4	G_2
dim $\mathfrak{g}$	$d(d+2)$	$d(2d+1)$	$d(2d+1)$	$d(2d-1)$	78	133	248	52	14

It is well known (see [Car, Ch. 11]) that each of the simple classical groups

$$A_d(q), {}^2A_d(q), B_d(q), C_d(q), D_d(q), {}^2D_d(q)$$

has a matrix representation as a subgroup of $PSL_{2d+1}(q^2)$.
In addition, the above table indicates that the exceptional groups

$$E_6(q), E_7(q), E_8(q), F_4(q), G_2(q)$$

are subgroups of $SL_{248}(q)$ (via the adjoint representation on the corresponding Lie algebra), so for the untwisted groups we can take $c = 31$.

Each twisted group G is the set of fixed points of some automorphism of the corresponding untwisted group, hence a subgroup of some $SL_{cr}(q)$ (or $PSL_{cr}(q)$) for some c. For example,

$$^2F_4(q) < F_4(q^2) < SL_{52}(q^2) < SL_{104}(q).$$

One can check from the table above that $c = 31$, and this finishes the proof of Theorem 1.

5 Acknowledgments

This paper is part of the author's PhD thesis. The author is grateful to his advisor Prof. Alex Lubotzky for introducing him to the problem and for useful discussions. Thanks to Prof. Inna (Korchagina) Capdeboscq, Prof. Nati Linial, Prof. Avinoam Mann, Dr. Nikolay Nikolov and Prof. Aner Shalev for useful remarks. Thanks are also due to M. Berman for his careful reading and for the referee for his constructive suggestions and criticisms which helped me improve this paper.

References

[Be] G. Birkhoff, On the structure of abstract algebras. Math. Proc. Cambridge Philos. Soc. **31** (1935), 433–454.

[BMP] A. Balog, A. Mann and L. Pyber, Polynomial index growth groups. Internat. J. Algebra Comput. **10** (2000), no. 6, 773–782.

[Car] R.W. Carter, Simple groups of Lie type. Pure and Applied Mathematics, Vol. **28**. John Wiley and Sons, 1972.

[CM] J. Cossey and S. O. Macdonald, A basis for the laws of PSL(2, 5). Bull. Amer. Math. Soc. **74** (1968) 602–606.

[CMS] J. Cossey, S. O. Macdonald and A. P. Street, On the laws of certain linear groups. Bull. Amer. Math. Soc. **75** (1969) 361–363.

[GHSSV] A. Gamburd, S. Hoory, M. Shahshahani, A. Shalev and B. Virag, On the girth of random Cayley graphs. Random Structures and Algorithms, **35** (2009), no. 1, 100–117.

[GLS] D. Gorenstein, R. Lyons and R. Solomon, The classification of the finite simple groups. vol. **3**. American Mathematical Society, 1998.

[Jon] G. A. Jones, Varieties and simple groups. J. Austral. Math. Soc. **17** (1974), 163-173.

[KL] P. Kleidman and M. Liebeck, The subgroup structure of the finite classical groups. LMS 129. Cambridge University Press, Cambridge, 1990.

[Lar] M. Larsen, Word maps have large image. Israel J. Math. **139** (2004), 149–156.

[LS] M. Larsen and A. Shalev, Word maps and Waring type problems. J. Amer. Math. Soc. **22** (2009), no. 2, 437–466.

[Lh] H. Lüneburg, Some remarks concerning the Ree groups of type (G_2). J. Algebra **3** (1966) 256-259.

[LN] R. Lidl and H. Niederreiter, Finite fields. Encyclopedia of Mathematics and its Applications, **20**. Addison-Wesley Publishing Company, MA, 1983.

[Ma] W. Magnus, Residually finite groups. Bull. Amer. Math. Soc. **75** (1969), 306-316.

[Ne] H. Neumann, Varieties of groups. Springer-Verlag New York, 1967.

[Ni] N. Nikolov, A product of decomposition for the classical quasisimple groups. J. Group Theory **10** (2007), no. 1, 43–53.

[NS1] N. Nikolov and D. Segal, On finitely generated profinite groups, I: Strong completeness and uniform bounds. Ann. of Math. **165** (2007), no. 1, 171-238.

[OP] S. Oates and M. B. Powell, Identical relations in finite groups. J. Algebra, **1**, no. 1, 11-39 (1964).

[Sh] A. Shalev, Word maps, conjugacy classes, and a noncommutative Waring-type theorem. Ann. of Math. **170** (2009), no. 3, 1383–1416.

[So1] B. Southcott, A basis for the laws of a class of simple groups. J. Austral. Math. Soc. **17** (1974), 500–505.

[So2] B. Southcott, Two-variable laws for a class of finite simple groups. Bull. Austral. Math. Soc. **10** (1974), 85–89.

[Ti] J. Tits, Les groupes simples de Suzuki et de Ree. Séminaire Bourbaki, **13** (1960-1961), exposé 210.

[We1] T. S. Weigel, Residual properties of free groups. J. Algebra **160** (1993), no. 1, 16–41.

[We2] T. S. Weigel, Residual properties of free groups. II. Comm. Algebra **20** (1992), no. 5, 1395–1425.

[We3] T. S. Weigel, Residual properties of free groups. III. Israel J. Math. **77** (1992), no. 1-2, 65–81.

Einstein Institute of Mathematics, The Hebrew University of Jerusalem.
current: Department of Mathematics, Weizmann Institute of Science.
and
Computer Science Division, The Open University of Israel.
E-mail address: uzy.hadad@gmail.com